

EVOLUTION OF COMPUTER VIRUSES

	First Generation	Second Generation
Language	Assembly language	Scripting language
Distribution Form	Binary	Source
Host Platform	CPU and OS	Source
Host Object	Executable codes	Documents
Propagation Media	Physical media	Network

FIG. 1
(PRIOR ART)

VIRUS DETECTION AND IDENTIFICATION

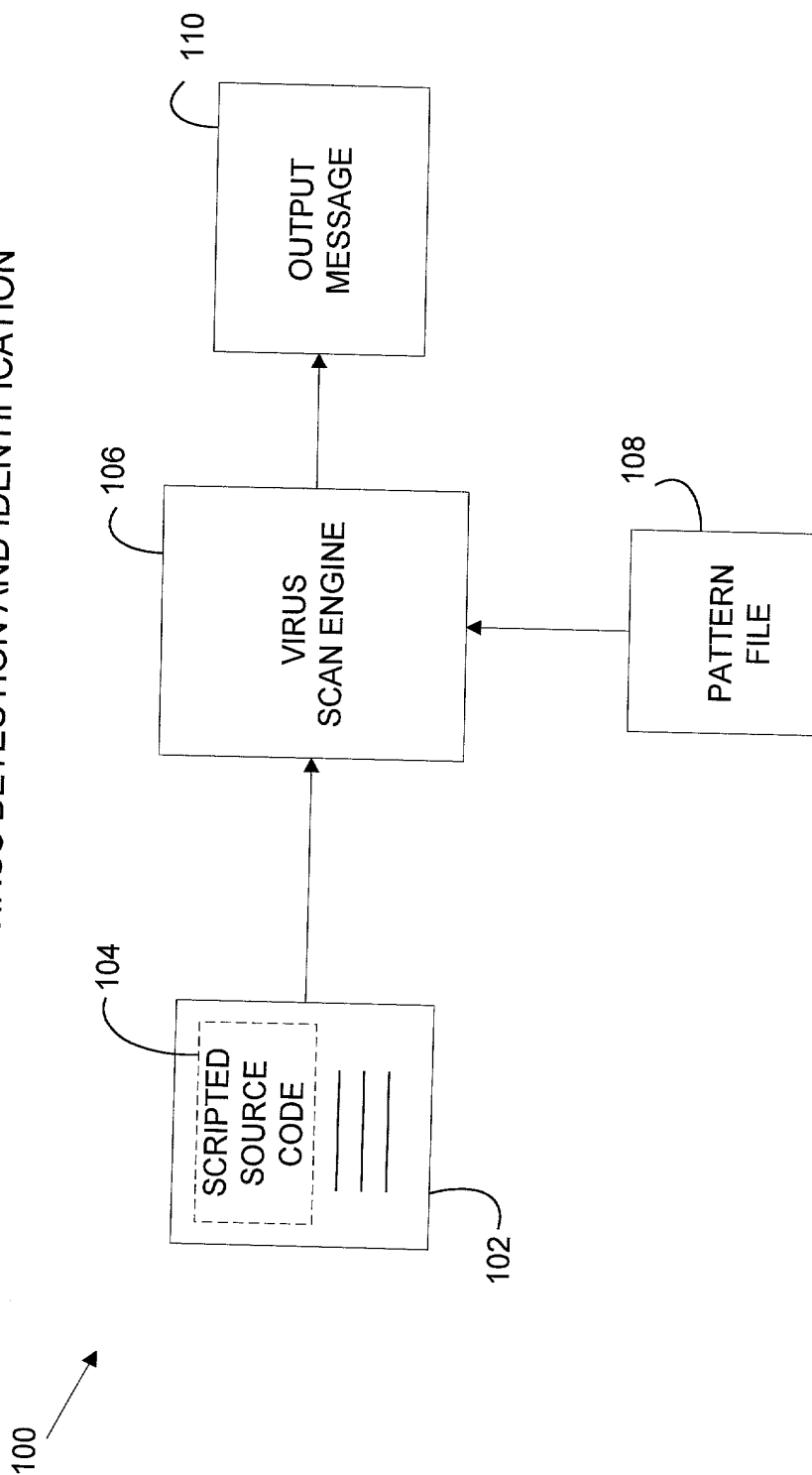


FIG. 2
(PRIOR ART)

SCRIPTING VIRUS SCAN ENGINE

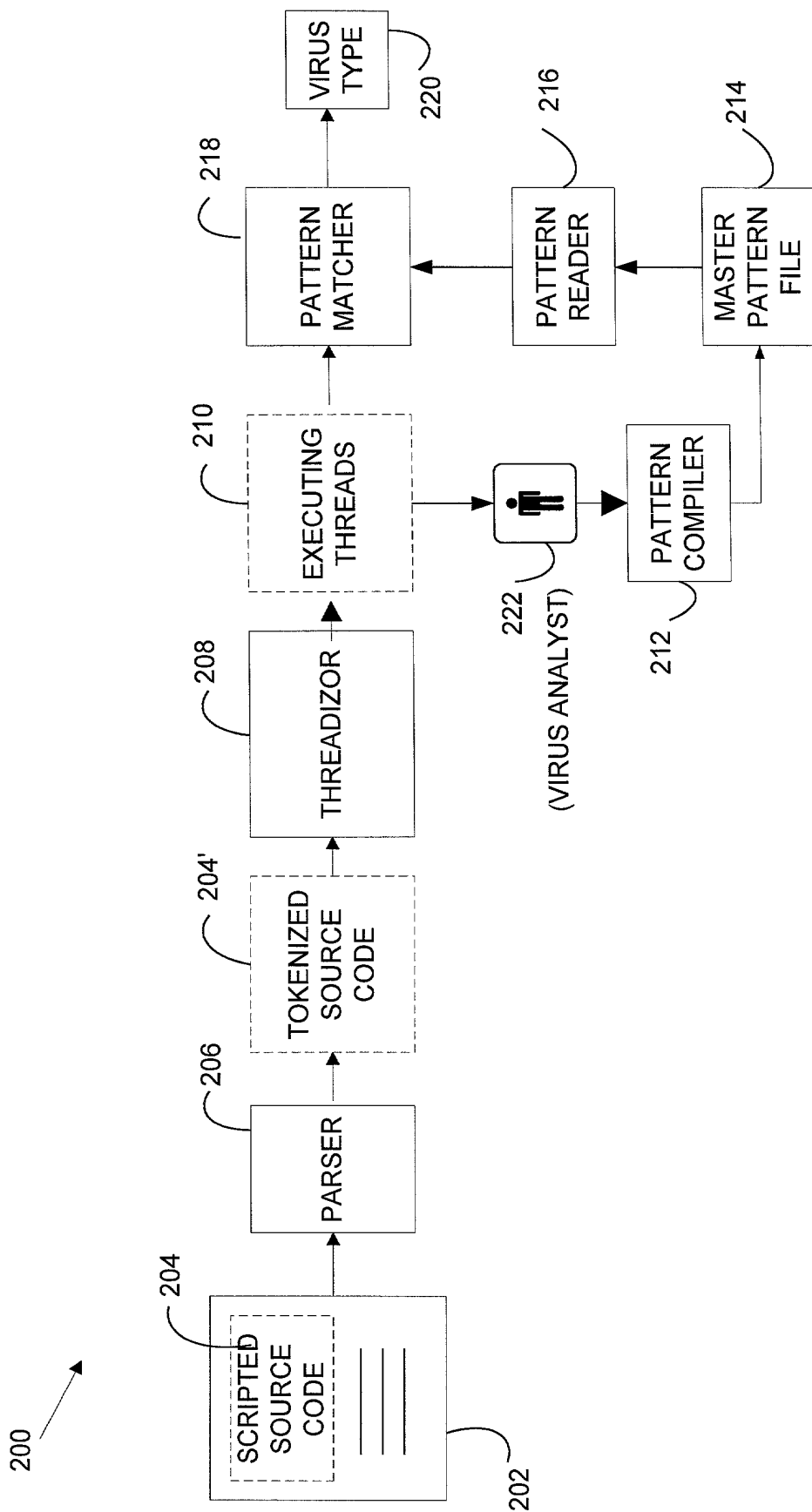


FIG. 3

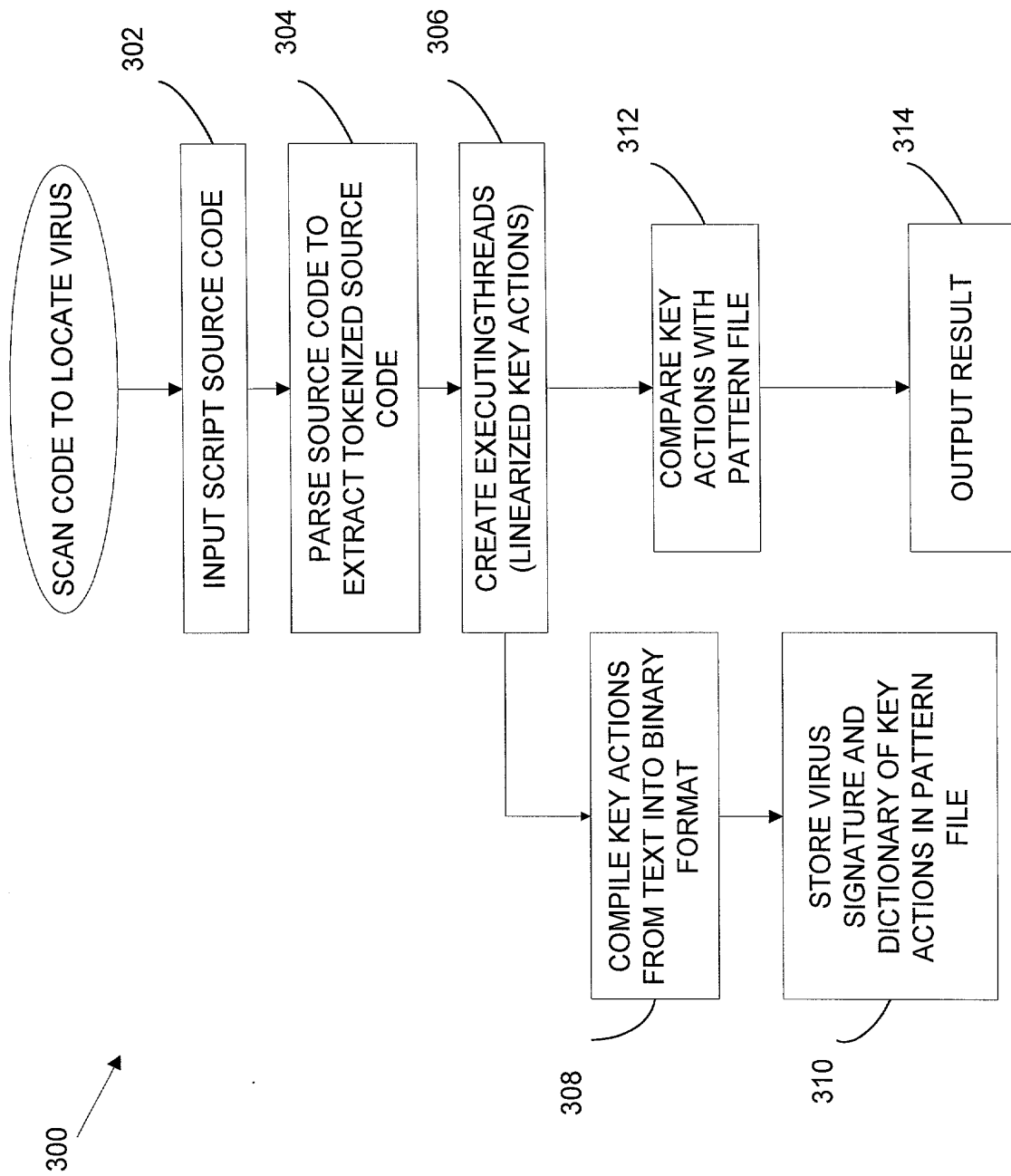


FIG. 4

SCRIPT SOURCE CODE

```
Private fso
Sub F1
Set file =fso . OpenTextFile ("your bank account", ForReading, True)
str = file . ReadLine
file . Close ( )
End Sub

Sub F2
Set file =fso . CreateTextFile ("c:\autoexec.bat", True )
file . WriteLine ("format c:")
file . Close ( )
End Sub

On Error Resume Next
Set fso=CreateObject ("Scripting.FileSystemObject")
Call F1
Call F2
```

FIG. 5A

TOKENIZED SOURCE CODE

```
Private fso
Sub F1
Set file = fso . OpenTextFile ( "your bank account" , ForReading , True )
str = file . ReadLine
file . Close (  )
End Sub

Sub F2
Set file = fso . CreateTextFile ( "c:\autoexec.bat" , True )
file . WriteLine ( "format c:" )
file . Close (  )
End Sub

On Error Resume Next
Set fso = CreateObject ( "Scripting.FileSystemObject" )
Call F1
Call F2
```

FIG. 5B

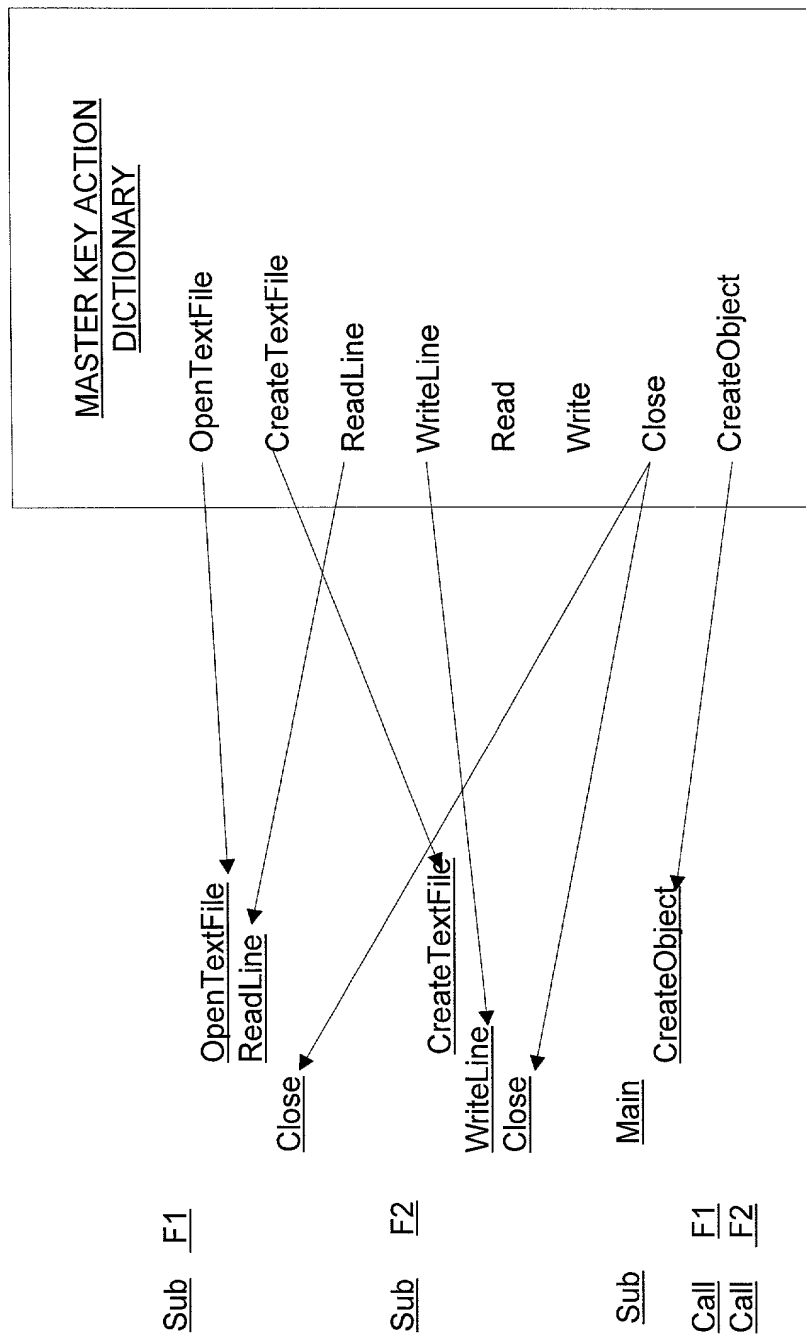


FIG. 6

LINEARIZED KEY ACTIONS

Sub Main

CreateObject
OpenTextFile
ReadLine
Close
CreateTextFile
WriteLine
Close

FIG. 7

PATTERN FILE

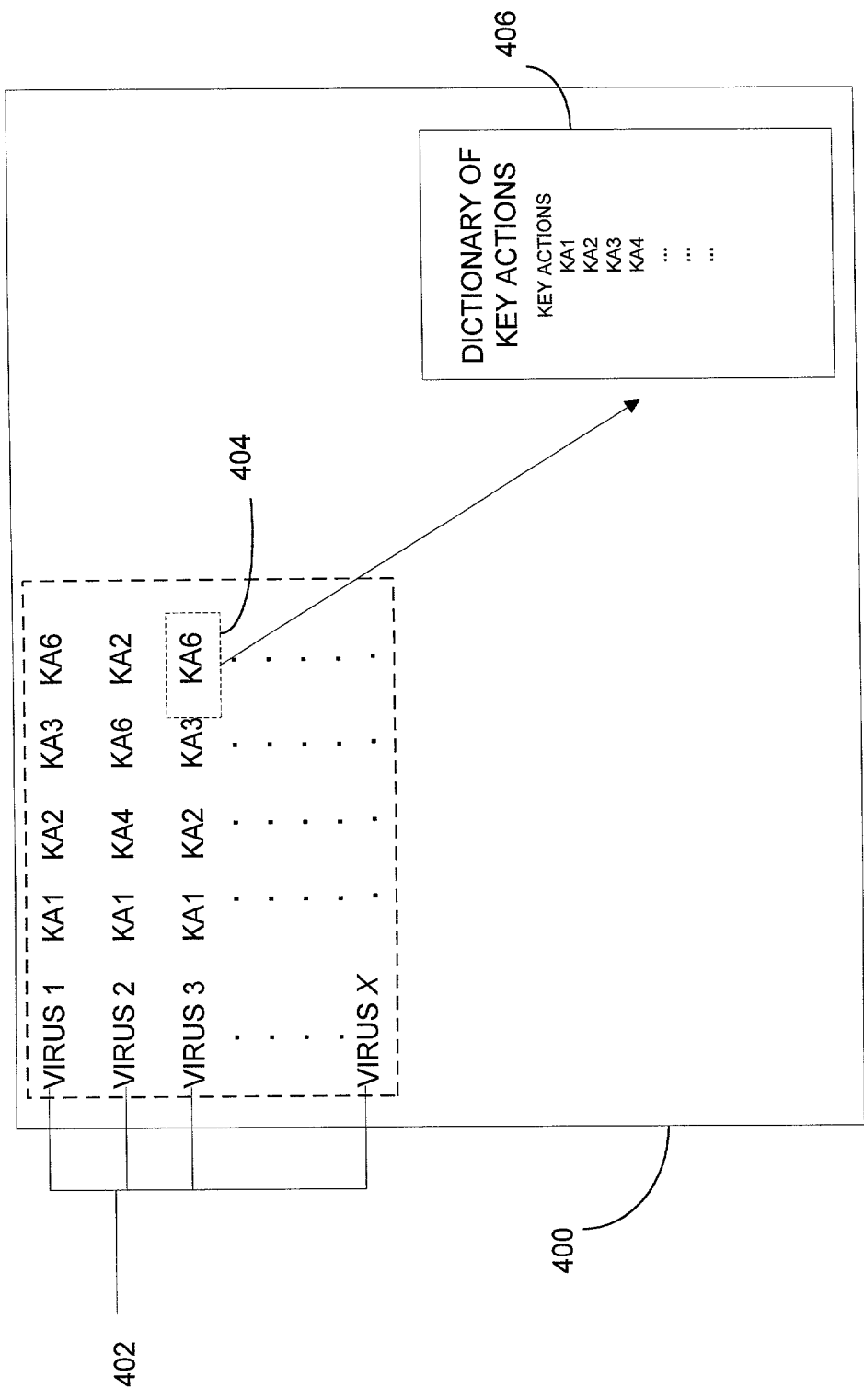


FIG. 8

POLYMORPH SCRIPT SOURCE CODE

```
Private obj
Sub Func2
Set file = obj.CreateTextFile ("c:\autoexec.bat", True )
file . WriteLine ("format c:")
file . Close ( )
End Sub

Sub F1
Set file = obj . OpenTextFile ("your bank account", ForReading, True)
str = file . ReadLine
file . Close ( )
End Sub

On Error Resume Next
Set obj = CreateObject ("Scripting.FileSystemObject")
Call F1
Call Func2
```

FIG. 9A

TOKENIZED POLYMORPH SOURCE CODE

```
Private obj
Sub Func2
Set file = obj . CreateTextFile ( "c:\autoexec.bat" , True )
file . WriteLine ( "format c:" )
file . Close ( )
End Sub

Sub F1
Set file = obj . OpenTextFile ( "your bank account" , ForReading , True )
str = file . ReadLine
file . Close ( )
End Sub

On Error Resume Next
Set obj = CreateObject ( "Scripting.FileSystemObject" )
Call F1
Call Func2
```

FIG. 9B

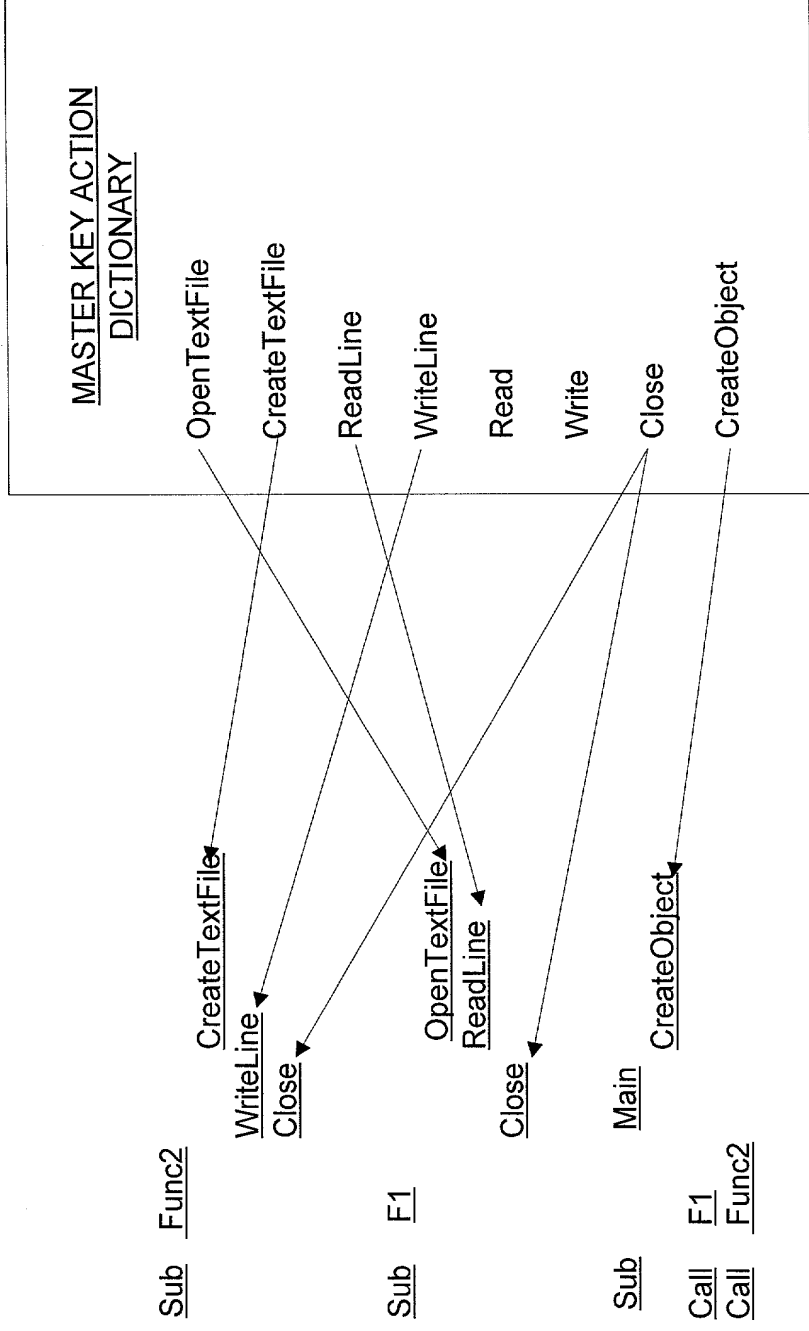


FIG. 10

LINEARIZED KEY ACTIONS OF POLYMORPH

Sub	Main
	CreateObject
	OpenTextFile
	ReadLine
	Close
	CreateTextFile
	WriteLine
	Close

FIG. 11

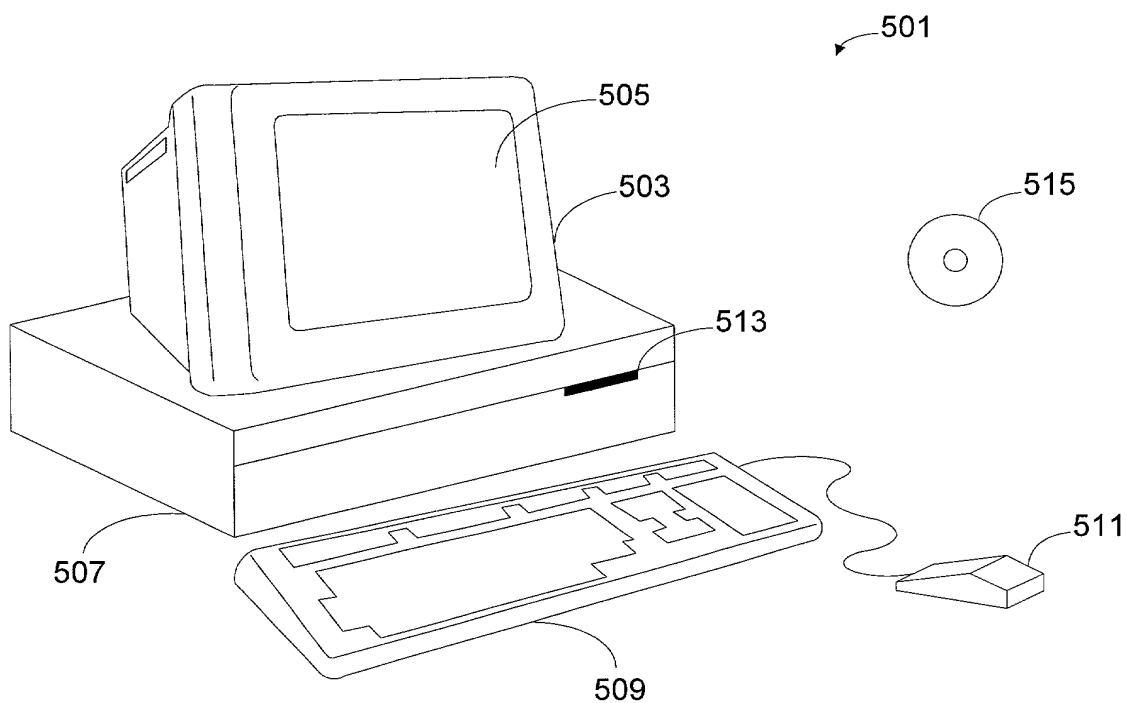


FIG. 12A

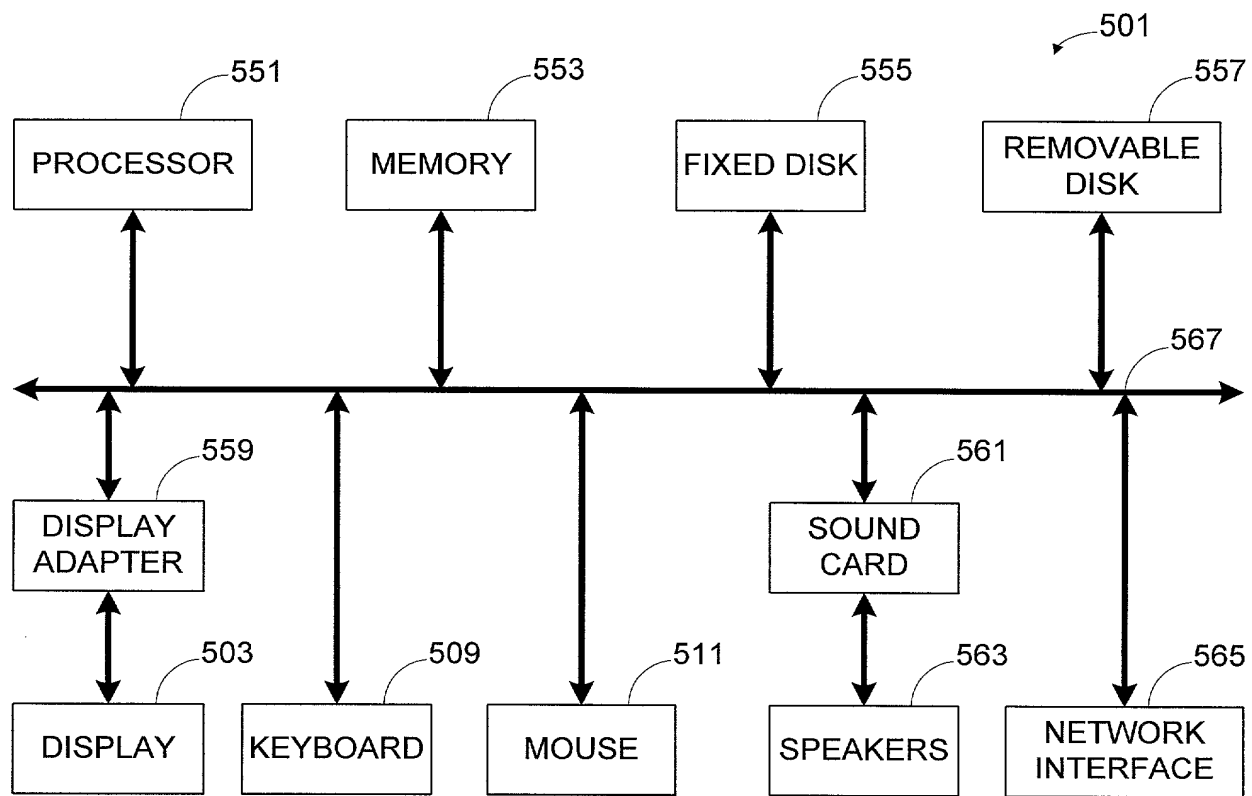


FIG. 12B